


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

SHA hash partial result compressing

1975

- 2004

Search

[Advanced Scholar Search](#)
[Scholar Preferences](#)
[Scholar Help](#)
Scholar [All articles](#) - [Recent articles](#) Results **1 - 10** of about **368** for **SHA hash partial result compressing**. (0.14 seconds)

[Performance impact of data compression on virtual private network transactions](#)- [*princeton.edu](#) [PDF]

 JP McGregor, RB Lee - Local Computer Networks, 2000. LCN 2000. Proceedings. 25th ..., 2000 - [ieeexplore.ieee.org](#)

 ... authentication, connectionless integrity, and anti-replay service (a form of **partial** sequence integrity ... ESP uses keyed **hash** algorithms such as **SHA-1** and ...

[Cited by 20](#) - [Related articles](#) - [Web Search](#) - [All 12 versions](#)

[Security analysis of SHA-256 and sisters](#)

H Gilbert, H Handschuh - Lecture Notes in Computer Science, 2004 - Springer

 ... **SHA-384/512** **results** from the iteration of a 256 + 512-bit to 256-bit (resp. 512 + 1024-bit to 512-bit) **compression** function. The **hash** computations are the ...

[Cited by 49](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 3 versions](#)

[Keying hash functions for message authentication](#)- [*ucsd.edu](#) [PDF]

M Bellare, R Canetti, H Krawczyk - Lecture Notes in Computer Science, 1996 - Springer

 ... than showing security against a **partial** list of possible attacks ... in current candidates like MD5 and **SHA-1**. (In ... MACs if one assumed the **hash** functions behaved ...

[Cited by 664](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 39 versions](#)

[\[PDF\] *The cryptographic hash function RIPEMD-160](#)

 B Preneel, A Bosselaers, H Dobbertin - CryptoBytes, 1997 - [cosic.esat.kuleuven.be](#)

 ... of FIPS 180, under the name **SHA-1**, which ... cryptanalytic work on the MD4-type **hash** functions. ... as RIPEMD was designed to withstand the **partial** attacks developed ...

[Cited by 32](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 4 versions](#)

[\[PDF\] *On the security of dedicated hash functions](#)

 B Van Rompay, B Preneel, J Vandewalle - SYMPOSIUM ON INFORMATION THEORY IN THE BENELUX, 1998 - [cosic.esat.kuleuven.be](#)

 ... the designs of the new ISO/IEC standards **SHA-1** and ... this change that allows the first **partial** attack on ... is of no practical importance for normal **hashing** but it ...

[Cited by 3](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 7 versions](#)

[Differential collisions in SHA-0](#)- [*sailams-u.ac.jp](#) [PDF]

F Chabaud, A Joux - Lecture Notes in Computer Science, 1998 - Springer

 ... the **compression** function, from which collision on the **hash** function are ... The first step of **SHA-0** is to perform an ... The **result** of this expansion is given by the ...

[Cited by 155](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 7 versions](#)

[Cryptanalysis of block ciphers based on SHA-1 and MD5](#)- [*m-js.com](#) [PDF]

MJO Saarinen - Lecture notes in computer science, 2003 - Springer

 ... 25 – 28, where we perform a **partial** meet-in ... that have been directly derived from dedicated **hash** functions. Section 2 discusses slide attacks against **SHA-1** and ...

[Cited by 21](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 8 versions](#)

[New constructions for secure hash functions](#)- [*psu.edu](#) [PDF]

W Aiello, S Haber, R Venkatesan - Lecture Notes in Computer Science, 1993 - Springer

 ... that we propose first stretch the input string mildly, and then **compress** the **result** of this ... We show how to use popular **hash** functions like MD5 or **SHA-1** to ...

[Cited by 9](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

[PDF] *Fast hashing on the Pentium

A Bosselaers, R Govaerts, J Vandewalle - Lecture Notes in Computer Science, 1996 - cosic.esat.kuleuven.be
... one exception: **SHA-1**. The rotations in **SHA-1** are, in contrast to the other **hash**
functions, confined to ... But even here the gain is only **partial**: pairing two ...

[Cited by 62](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 28 versions](#)

[CITATION] CRUSH: A new cryptographic hash function using iterated halving technique

P Gauravaram, W Millan, L May - Proceedings of the workshop on Cryptographic Algorithms and ..., 2004

[Cited by 13](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Key authors: [M Bellare](#) - [P Rogaway](#) - [R Canetti](#) - [H Krawczyk](#) - [M Cai](#)

Google

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

SHA hash partial result compressing

Search

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2009 Google